BILETA
British & Irish Law, Education and Technology Association
2007 Annual Conference
Hertfordshire 16-17 April
UH

Radio Frequency Identification Technology (RFID): Malaysia's privacy at the crossroads?

Noriswadi Ismail[1]
British Chevening Scholar, University of Strathclyde
Email: noriswadi.ismail@strath.ac.uk

1 Introduction

Back 1998, the Kuala Lumpur International Airport[2] had deployed the Malaysian ePassport autogate system. The technology requires Malaysian travellers to place their ePassport document on the autogate slot, followed by verification of their fingerprints on a biometric scanner. The time to scan and verify the passport owner takes less than ten second to complete. The system also does a check against a watch-list on the server to detect any criminal suspects trying to enter Malaysia. The government had also initiated the usage of RFID passports – claimed to be the first in South East Asian region and the world.[3] RFID chips which are embedded in these Malaysian passports possess strong capability to expose personal information and trail the historical data of a traveller's journey.[4] Invariably, the motivation implementing these ePassport and RFID passports initiatives are meant for surveillance. It also evidences the government's level of seriousness to combating potential terrorism and crimes.

Alas, after eleven years of technology deployment, there have been mixed reactions by the Malaysian citizens. On one hand, technology proponents viewed that these developments have moulded the growth of Malaysia's Multimedia Super Corridor[5], and thus, charting the progress towards Vision 2020 or locally translated to *"Wawasan 2020."*[6] On the other hand, privacy proponents viewed that much could be done to addressing privacy concerns in Malaysia despite of the RFID technology.[7] Due to these divided views, this paper proposes to outline a cursory RFID technological explanation and explore the approaches adopted by the United Kingdom and the European Union. The central focus will be on the predictions to Malaysia's RFID players once the Personal Data Protection (PDP) Bill would have been passed by the parliament. Primarily, three predictions are discussed:

- Readiness towards complying privacy and data protection regulations;
- Legal risk management strategy; and
- Pre-empted compliance cost strategy.

[1] HeiTech Padu Berhad, http://www.heitech.com.my; see also his RFID blog at http://the-rfid-nexus.blogspot.com.

[2] See generally http://www.klia.com.my/; see also http://en.wikipedia.org/wiki/Kuala_Lumpur_International_Airport, accessed 18 February 2007 and http://www.mida.gov.my/beta/view.php?cat=14&scat=1573, accessed 18 February 2007.

[3] See http://en.wikipedia.org/wiki/Malaysian_passport, accessed 18 February 2007.

[4] See generally http://www.ftc.gov/bcp/workshops/rfid/tien1.pdf, accessed 18 February 2007.

[5] See http://www.msc.com.my/, accessed 18 February 2007.

[6] See an interesting speech by the former Prime Minister, Tun Mahathir Mohammed, Malaysia's foremost Vision 2020 architect: http://unpan1.un.org/intradoc/groups/public/documents/apcity/unpan003222.pdf., accessed 18 February 2007; see Malaysian Dream: http://www.themalaysiandream.net/documents/12/vision-2020 accessed 20 February 2007; see also an analytical review by Gavin Stamp, BBC Reporter, BBC News, Malaysia *"Malaysia focused on 2020 Vision",* Thursday, 1 June 2006: http://news.bbc.co.uk/2/hi/business/5020794.stm, accessed 18 February 2007.

[7] See http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-545269, accessed 20 February 2007.

2 What is RFID?

RFID connotes Radio Frequency Identification Technology, a terminology which illustrates any system of identification wherein an electronic device that uses radio frequency or magnetic field variations to communicate is attached to an item.[8] There are two most-talked-about components of an RFID; Tag and reader respectively. Tag is an identification device attached to the item for tracking whilst reader is a device that can recognise the presence of RFID tags and read the information stored on them. The reader can then inform another system about the presence of the tagged items. The system with which the reader communicates usually runs software that stands between readers and applications. This software is called RFID middleware.[9]

The exact technology deployment date of RFID is relatively unknown. But, generally it goes back to 1920s during the World War II.[10] As the technology suggested, at that point of time, the all Identity Friend or Foe (IFF) system was used in British aircrafts. The IFF system comprised important components of *interrogator* and *transponder.* The interrogator was the radar system and the transponder was an unwieldy box of tubes with dials and switches. The term *interrogator* provides the guidance as to how the system worked: the ground station sent out a radar signal, and the transponder receiving this signal reflected it back, causing the radar antenna to receive a stronger return than it otherwise would have. The *transponder* also 'swept' the frequency of its return back and forth over a small range as it responded, causing the radar return to pulsate according to a specific rhythm. [11]

2.1 RFID functions and operations

RFID could not operate and function without frequency.[12] The operating frequency is the electromagnetic frequency the tag uses to communicate or to secure power. Due to the nature of RFID which broadcast electromagnetic waves, they are regulated as radio devices. Thus, RFID systems must not interfere with other existing protected applications such as emergency service radios or television transmissions. Throughout the world, regulatory bodies have chosen different ranges for ultra high frequencies (UHF) in different parts of the world. [13] Even if each country requires a different range of UHF, it is suggested that one possible global standard known as EPCglobal standard will be able to match varying local regulatory requirements.[14]

The tag and reader are the two key components to operate an RFID system. The reader functions as transmitter of the system which contains electronics that use an external power source to generate the signal that drives the reader's antenna. In turn, it creates the appropriate radio wave. The radio wave may be received by an RFID tag, which in turn

[8] *Bill Glover & Himanshu Bhatt,* "RFID Essentials" (2006, O'Reilly) pp 1-19; see also http://en.wikipedia.org/wiki/RFID, accessed 20 February 2007.

[9] *Ibid., Glover & Bhatt* fn 6 above at p. 1.

[10] *Ibid., Glover & Bhatt* fn 6 above at p. 59; see generally Matt Ward, Rob van Kranenburg and Gaynor Backhouse, *"RFID: frequency, standards and innovation",* JISC Technology and Standards Watch, May 2006 at p. 4-5. Retrievable online: http://www.jisc.ac.uk/uploaded_documents/TSW0602.pdf, accessed 20 February 2007.

[11] *Ibid., Glover & Bhatt*, fn 8 above at p. 59.

[12] RFID typically operates within a low frequency (LF), high frequency (HF), ultra high frequency (UHF) and microwave. In practice, the actual frequencies available to RFID are limited to those frequencies se aside as Industrial Scientific Medical (ISM). Frequencies lower than 135 kHz are not ISM frequencies, but in this range RFID systems are usually using powerful magnetic fields and operating over short ranges, so much so, interference is less of an issue than it might be otherwise.

[13] Battle for different applications of UHF is also still taking place amongst RFID users in specific industry such as pharmacy. See generally: http://www.unisys.com/commercial/news_a_events/all__news/04048642.htm, accessed 20 February 2007.

[14] It is argued that this standard shall lead to convergence and it is hoped that governments and standard bodies should make a genuine effort to cooperate producing a global standard; see also EPC Global, "Communications Commission sets the stage for the EU to realise benefits of applications based on EPCglobal standards" Retrievable online: http://www.epcglobalinc.org/about/media_centre/press_rel/Press_Release_Commission_Communication_on_RFID_070314.pdf, accessed 20 February 2007; see generally: http://en.wikipedia.org/wiki/EPCglobal, accessed 20 February 2007.

‘reflects’ some of the energy it receives in a particular way (based on the identity of the tag).[15] Whilst this reflection is going on, the RFID reader is also acting as a radio receiver, so that it can detect and decode the reflected signal in order to identify the tag.[16]

2.2 RFID types of categorisation

There are essentially three types of categorisation within an RFID system which is based on the power source used by the tag, as particularised:-

- *Passive tag* – This requires no power source at the tag. It does not require any batteries but utilises the energy of radio wave to effect its operation.[17] In this category, it results to the lowest tag cost at the expense of the performance. Example that could be seen in practice is the usage of passive tag in individual product items for applications in supermarket checkouts and smart cards[18];

- *Semi-passive tag* – This relies on the battery built into the tag in order to achieve a better performance within the operating range. In this category, the battery powers the internal circuitry during the communication; however it is not used to generate radio wave.[19] This tag is mostly fragile and expensive in the market[20]; and

- *Active tag* – It utilises batteries for their entire operation which can generate radio wave actively in the absence of a reader.[21] In this category, the tag is capable of a peer-to-peer communication. It has larger memory as compared to the passive tag, possesses higher processing capabilities and secure.[22]

Without any doubt, the semi-passive tag is the only category which does not require the involvement of a radio wave. It is also due to the costly price which compels the RFID provider to opt the first and second category.

3. RFID in Malaysia - a brief overview

Based on IDC’s forecast, the Malaysia’s RFID market is expected to hit RM77 million by 2010[23] with a compound of annual growth rate of 45.84%. Significant developments have

[15] Steve Hodges & Mark Horrison, *“WHITE PAPER – Demystifying RFID: Principles and Practicalities”*, Auto-ID Centre, Institute for Manufacturing, University of Cambridge, Published 1 October 2003 at p. 8-9; see also http://www.ifm.eng.cam.ac.uk/automation/publications/documents/CAM-AUTOID-WH024.pdf, accessed 20 February 2007.

[16] *Ibid.,* at p. 9.

[17] *Ibid.,* at p.9.

[18] See JISC Technology and Standards Watch, May 2006 at p. 4-5.

[19] *Ibid.,* at p.9.

[20] See fn 16 above, at p. 4-5.

[21] *Ibid.,* at p.9.

[22] See fn 18 above, at p.4-5.

[23] See http://www.theedgedaily.com/cms/content.jsp?id=com.tms.cms.article.Article_d2cc4b98-cb73c03a-29d65b00-cd5c3a50, accessed 20 February 2007 see also http://morerfid.com/details.php?subdetail=Report&action=details&report_id=1032&display=RFID, accessed 20 February 2007. In the Malaysia RFID 2006-2010 Forecast and Analysis, it predicted the state of the market for RFID solutions implementation in Malaysia, historical development, and prediction for the future. It also presents an end user's RFID case study and write-up on key players that offer RFID solutions in Malaysia. Based on the study, hardware comprises largest portion of the total commercial RFID spending in 2005 at 60%, driven primarily by the purchases of readers and tags, followed by software and services which take up the remaining 40% of the RFID spending. "Based on the IDC's definitions, software revenue captured in this forecast is limited to RFID middleware, reader firmware, and additional enterprise middleware directly related to integrating data from the RFID layer with the enterprise application layer. It does not incorporate spending on enterprise applications and upgrades beyond middleware to accommodate and take advantage of the influx of data from RFID tags. Services included in this forecast are business process consulting, installation, systems integration, and

taken place in Malaysia's RFID growth. On December 2006, the Malaysian Road Transport Department had initiated the usage of RFID license plates with the attempt to reduce the number of car thefts in the country. The plate will contain the information about the owner of the car and the vehicle. This will help the police official to know if the car has been stolen.[24] On 24 February 2007, Malaysia had released the world's smallest RFID microchip which measures between 0.4mm by 0.4mm with a built-in antenna, which can be embedded on paper.[25] The microchip, developed under the Malaysia Microchip Project, at a cost of US$50 million (RM180 million) based on Japanese technology, is the first with multi-band frequencies.[26] These developments envisage promising RFID growth in the Malaysian market and if the IDC analysis remains prevalent, it is predicted Malaysia will be the central RFID investment within the South East Asian region.

4. Does RFID undermine privacy and data protection?

4.1 Malaysia's cursory development

Arguably, many of these developments have posed significant privacy and data protection concerns not only in Malaysia but also throughout other jurisdictions.[27] In Malaysia, the effort to draft the PDP Bill started in 2000. However, until today, the legislation is yet to be seen.[28] Rumours claimed that the Bill that was introduced in 2000 was motivated by the European Union (EU) regulatory approach as compared to the self-regulation approach of safe harbour of the United States.[29] But now, the situation is otherwise and it has given quite a general setback to various industries in implementing possible data protection and privacy strategy within their organisations.

Recently, the issue of the PDP Bill delay has been mentioned in the parliament. One of the members of parliament lamented that the government was taking too long to pass laws on personal data protection, which existed in ninety countries. He further viewed that it is imperative that Malaysia hasten the enactment of the law and poignantly added that it could affect efforts to sustain Malaysia's position as a competitive outsourcing country after India and China.[30] The moans and groans are not only commonly shared by the Malaysian public but also multinational corporations and foreign investors. The next question to be asked is

ongoing support services. Software and services would pose more growth potential, with CAGR of 48% and 51% respectively.

[24] The owner of the car should be nearby if the police officials want to check the driver's identity. The system will be implemented next year. The new cars would have such plates followed by the older ones. The risk what I see is that in case the RFID system of your car breaks down then you might be pulled from your car by the cops thinking that you are a thief. See generally http://www.iht.com/articles/ap/2006/12/09/asia/AS_GEN_Malaysia_Car_Thefts.php, accessed 22 February 2007.

[25] See http://www.hitachi.co.jp/Prod/mu-chip/index.html, accessed 22 February 2007.

[26] The Prime Minister, Datuk Seri Abdullah Ahmad Badawi, who launched the microchip yesterday, said the chip with its identification serial number, could help to counter the forgery of government documents; currency notes; halal certificates; medical products and compact discs, among others. Besides, some applications currently being developed would further assist to improve the public service delivery system. See http://www.mida.gov.my/beta/view.php?cat=14&scat=1552, accessed 22 February 2007; see also http://en.qschina.com/html/tradeinfo/html/2007/3/13/9088.html, accessed 22 February 2007.

[27] See the ongoing consultation effort by the European Union: http://www.rfidconsultation.eu/, accessed 22 March 2007.

[28] See Ida Madieha Azmi, "E-commerce and privacy issues: an analysis of the personal data protection bill", *International Review of Computer Laws & Technology,* Volume 16, No. 3, pp 317-330, 2002; see also

[29] See Ida Madieha Azmi, "Why has data protection law been delayed in Malaysia? Nothing to do with Islam and who needs it anyway?" BILETA 2006, Malta 6th – 7th April 2006. See generally: http://events.um.edu.mt/bileta2006/29DP&I%20v1%20Ida%20madieha%20Aziz.pdf, accessed 22 February 2007; see also Hurriyah El Islamy, "Privacy and Technology", BILETA 2005, Belfast retrievable at: http://www.bileta.ac.uk/Document%20Library/1/Privacy%20and%20Technology.pdf, accessed 22 February 2007.

[30] Jane Ritikos, Florence A. Samy and Elizabeth Looi, "Same law apply for bloggers, say BN rep", The Star Online, Thursday March 22 2007; see also: http://star-techcentral.com/tech/story.asp?file=/2007/3/22/technology/20070322114048&sec=technology, accessed 22 March 2007.

whether the RFID technology undermines privacy and data protection? There are two possible and skeletal answers. First, in the event the Bill has analysed thoroughly the application of emerging new technology and its convergence[31] *vis-à-vis'* the privacy and data protection provisions, it is believed it would not generally undermine due to its technology neutrality approach. Second, in the event the Bill has not achieved the same, a secondary review to the existing draft should be made pedantically. However, it should be noted that these answers may be duly substantiated once the Bill takes place in Malaysia.

4.2 The EU reaction – a brief overview

Within the EU, the Article 29 Working Party which has been established under Article 29 of Directive 95/46/EC articulates existing privacy and data protection issues.[32] On the data protection front, the Working Party has mooted its concerns on the effect of RFID technology which may lead to violation of human dignity and data protection rights. The focus of the concern surrounds on the possibility of businesses and governments which have deployed RFID and thus, leads to prying into the privacy sphere of individuals. [33] Based on the published summary of the responses, RFID stakeholders deemed to be satisfied with the working document. In practice, many may assert that the examples of RFID applications illustrated in the working document do not reflect the reality.[34] It is argued that societal benefits and realistic appreciation of technical possibilities should be inferred whilst analysing RFID applications.

Primarily, two governing Directives apply within the EU; Directive 95/46/EC on the protection of personal data and Directive 2002/58/EC on the protection of personal data in the electronic communications sector. These directives provide the mechanism of data processing to be adhered by the member states with some restrictions. [35] Upon reading the provisions under the Directive 95/46/EC, it could be generally summarised that not all RFID applications are governed under the provisions. This is due to the nature of RFID technology itself, i.e. via RFID tags and the complex technicality involved. The tags possess the capability to exchange information and thus, the provisions fail to achieve its technology neutrality approach, leading to a level of biasness towards existing RFID technical solutions and also other related technology. i.e., Ambient Intelligence (AmI).[36]In Directive 2002/58/EC, services must provide continually the possibility, of using a simple means and free of charge, of temporarily refusing the processing of certain personal data for each communication. It is argued however, a PC based system would fulfil the needs of the provision, but RFID and AmI will fail to comply with the spirit due to the nature of its technical interface.[37]

[31] See generally http://en.wikipedia.org/wiki/Technological_convergence, accessed 22 March 2007.

[32] See generally http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/index_en.htm; see also http://www.edri.org/edrigram/number3.3/consultation, and http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp105_en.pdf respectively, accessed 22 March 2007.

[33] See Olli Pitkanen and Marketta Niemela, "Privacy and data protection in emerging RFID-applications", Helsinki Institute for Information Technology HIIT, Helsinki University of Technology and University of Helsinki, VTT Technical Research Centre of Finland. This paper was presented in the EU RFID Forum 2007, retrievable at: http://www.rfidconvocation.eu/Papers%20presented/Business/Privacy%20and%20Data%20Protection%20in%20Emerging%20RFID-Applications.pdf, accessed 22 March 2007.

[34] *Ibid.,* see fn 31 above, at p.1-2.

[35] The data should be processed fairly and lawfully; collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes; adequate, relevant and not excessive in relation to the purposes; accurate and, where necessary, kept up to date. For restrictions, see http://ec.europa.eu/justice_home/fsj/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf, accessed 22 March 2007.

[36] Concept of Ambient Intelligence (AmI) is described as a vision where humans are surrounded by computing and networking technology unobtrusively embedded in their surroundings. AmI puts the emphasis on user-friendliness, efficient and distributed services support, user empowerment, and support for human interactions. This vision assumes a shift away from PCs to a variety of devices which are unobtrusively embedded in our environment and which are accessed via intelligent interfaces using RFID, PDA, wearables and robots.

[37] *Ibid.,* see fn 31 above, at p.2-4.

4.3. The UK reaction – a brief overview

In the UK, the Data Protection Act 1998 concerns the processing of personal data. The Data Protection Technical Guidance Radio Frequency Identification has outlined two scenarios in which personal data might be processed using RFID.[38] First, personal data may be stored on the tags themselves, or linked to a database containing personal data. Second, if tags on individual items can be used to identify the individual associated with the item, they will be personal data.[39] Alike of the EC Directives' provisions, the guidance mentioned that where personal data is collected, generated or disclosed using RFID either directly or indirectly, the Act will apply. In addition, RFID users should apply the data protection principles of fair processing, use limitation, data quality, data retention and security.[40] The guidance has also mentioned extensively specific data protection concerns which involve security, monitoring, profiling and technical solutions.[41]

Besides the guidance, it could be seen that the UK Information Commissioner has put a very high concern on the level of the UK's surveillance society. In a report on surveillance society, by the Surveillance Studies Network[42], RFID has been cited as one of the central issues and discussions. Even if the report does not critically analyse the technical aspects of RFID and its dangers to privacy and surveillance in detail, it has however outlined future directions to the data protection actors whenever potential RFID issues take place. It is also noteworthy to mention that the report has painstakingly analysed various social, technical, regulatory and economic perspectives which could be applied in today's context in achieving a balanced surveillance society. It is convinced the substantive analysis of the report should be able to guide Malaysia's roadmap in the event potential surveillance and privacy concerns will be raised subsequent to the passing of PDP Bill.

5. Predictions for Malaysia

On 28 January 2007, Council of Europe had historically celebrated the first ever Data Protection Day.[43] It was the occasion for European citizens to become more aware of personal data protection and of what their rights and responsibilities are in that regard. That initiative is considered as a considerable breakthrough platform to disseminate the significance of data protection not only to European citizens, but also providing a model to the rest of the world to adopt the similar approach and strategy. After years of legislative measures and harmonisation within the EU, it could be generally said that the level of regulatory harmonisation between the member states has been quite effective and fruitful.

[38] See http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/radio_frequency_indentification_tech_guidance.pdf, see also http://www.ico.gov.uk/global/search_results.aspx?search=RFID, accessed 22 March 2007.

[39] *Ibid.,* see fn 36 above at p 3-4.

[40] *Ibid.,* see fn 36 above, at p.4.

[41] The concerns include "skimming", "hacking", "rogue RFID tag readers", "skimmers" "cloned EFID chip", "blocker tags" and "clipped tags". For more detailed explanation, see the guidance at p. 5-7; see also http://www.ico.gov.uk/upload/documents/library/data_protection/introductory/radio_frequency_identification_tags.pdf, accessed 23 March 2007.

[42] As the bulk report remains an authoritative and guidance to data controller, it is suggested however that the substance of the report should be inferred within the context of data protection strategy and management of the data controller. See http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/surveillance_society_full_report_2006.pdf, accessed 23 March 2007; see also the appendices of the report: http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/surveillance_society_appendices_06.pdf, accessed 23 March 2007; see the summary of the report: http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/surveillance_society_summary_06.pdf, accessed 23 March 2007.

[43] See http://www.coe.int/t/e/legal_affairs/legal_co-operation/data_protection/Data_Protection_Day_default.asp#TopOfPage, accessed 23 March 2007; see generally http://ec.europa.eu/idabc/en/document/6526/194, accessed 23 March 2007.

To the contrary, Malaysia is facing potential challenges to co-exist the issue of privacy, data protection and RFID simultaneously, notwithstanding the PDP Bill delay. [44] As to move forward, it is submitted that Malaysia needs potential predictions to accelerate the already existing problems, challenges and directions that privacy and data protection have posed to RFID. There are three predictions that could be mapped and guided in the near future; readiness to complying with the privacy and data protection regulations, legal risk management strategy and pre-empted compliance cost and strategy. These predictions are hypothesised from the EU and the UK data protection historical legislative and consultation experience, literature, industries' approaches, technical and security approaches as well as the ongoing EU RFID public consultation.[45]

5.2 Readiness to comply

Issue of readiness is the main concern whenever a specific legislation takes place. In the context of RFID and privacy, it could be seen that the readiness is a shared responsibility by the RFID players.[46] Leading solution providers in the UK and EU[47] had taken the necessary steps to ensure technology would be able to provide reasonable preventive measure especially when dealing with privacy and data protection issues.[48] RFID evaluation is considered as the best practice to instil the readiness. The evaluation will cover an extensive assessment on RFID technology and affiliating the assessment with privacy and data protection provisions. The RFID evaluation will be able to provide the roadmap to the players towards complying with privacy and data protection provisions. As RFID evaluation needs involvement within a particular organisation or company which is deemed to be multi departmental. In this regard, a proposed RFID privacy and data protection team should be established to ensure that the deployment of RFID technology is technically compliant, with the privacy and data protection provisions and there should be a continuous assessment and self regulation effort to ensuring effectiveness in implementation.

It is argued that the establishment of such a team would lead to issues of cost and resources. However, to debunk that, the readiness should be embarked on by the organisation via clear terms of reference for a particular organisation or company. For example, a Director in semi medium enterprises could outline brief and understandable privacy and data protection terms and conditions, being part and parcel of the company's privacy policy. This policy should be able to explain certain emerging new technology deployment such as RFID and how it would be privacy friendly within the context of data protection provisions. Dynamically, dissemination through peer-to-peer knowledge management sharing session shall be an added value in a long run. Further, for companies which are directly and indirectly deploying the RFID technology, middleware and applications, it is essential for these companies to conduct effective road show and continuous compliance briefing within their companies and to the Malaysian public in ensuring business continuity.[49] These companies may admit that such effort of dissemination and diffusion requires a dedicated timeline. Besides, these companies' substantial investment may also add towards their marketing and branding initiative by taking into account their commitment of compliance. Thus, it is submitted that having a dedicated compliance team to manage RFID and privacy related issues are exceedingly desirable.

[44] See fn 28 above.

[45] See fn 25 above.

[46] For the purpose of this paper, RFID player means the service provider, the regulator, the customers who are deploying RFID and the general public who have direct and indirect affiliation with RFID technology, applications and middleware.

[47] See generally the position paper: http://www.rfid-in-action.eu/public/papers-and-documents/guidelines.pdf, accessed 24 March 2007.

[48] One of the examples is SAP, see generally SAP approach: http://www.sap.com/netherlands/industries/healthcare/pdf/SAP_RFID_for_healthcare_readiness_check.pdf, accessed 24 March 2007.

[49] Business continuity is a standard which is applied globally in managing continuous business process. Further details could be read here: http://www.thebci.org/gpg.htm, accessed 24 March 2007; se also a guide for business continuity guide: http://www.axa4business.co.uk/resources/files/BizContinuityGuideT1404.pdf, accessed 24 March 2007.

It is also argued that the readiness to comply with the terms involve bilateral diffusion between Malaysian proposed regulator; Data Protection Commissioner/Privacy Commissioners/Information Commissioners and the RFID industry. The proposed regulator should be able to gauge and balance the industry's understanding, growth and challenges besides imposing compliance mechanism to uphold privacy and data protection. In order to avoid over excessive compliance and regulatory mechanism, such technology neutrality approach should be adopted by collating the industry's feedback and analysing the expected maturity and growth of RFID related privacy issues. For example, one of the key steps that have been taken by the Office of Communications (Ofcom), UK is the deregulation of RFID. Ofcom has allowed the use of RFID technology without the need for a licence. The rationale of deregulation is influenced by the need to remove unnecessary regulatory obligations upon industry.[50] The step taken has balanced the RFID growth which encourages RFID market maturity. Besides Ofcom, as reiterated, the UK Information Commissioner technical guidance is a leading example to display that the regulator could do more instead of excessive regulatory compliance.[51]

5.3 Legal risk management strategy

Business continuity has always been the life cycle of organisations and companies. The term 'legal risk management'[52] is neither a new nor a coined terminology. It is however, a hybrid approach or strategy assessing issues within the application of risk management module and legal principles.[53] Due to the hybrid nature of the module, similar to the RFID technology, RFID players should be able to preach a strong risk management culture clearly and understandably. A strong risk management culture starts with these levels of risks' process: risk identification, risk analysis, risk profiling, risk mitigation, risk control and risk scorecard.[54] The traditional approach of risk management is mostly centred upon internal auditing exercise and internal control of organisations and companies. However, as the global market matures, risk management has been extended to control or pre-empted specific problems and issues, in the absence of a clear legislation and standard. Ultimately, the aim of having a legal risk management strategy for RFID players is to complement the players' readiness in complying privacy and data protection provisions.[55]

Legal risk management does not favour any organisations or companies but it complements these entities within their risk appetites. There is an indispensable strategy that Malaysian RFID players can strategise whilst awaiting the PDP Bill to be passed by the Parliament. The strategy relies on the need to establish RFID risk manual.[56] This manual will be able to outline brief technical illustration of the RFID usage, the sensitivity areas that lead to privacy issues as well as how to mitigate and manage the RFID and privacy related risk perceptions. The manual should also provide the commitment to manage the risk and at the same time, eliminating the risk that would have been derived from RFID middleware, applications and deployment. It is submitted that the manual should take into various aspects which include, cost, technical, legal, research & development, liability, operations, third party and reputation.

[50] See Ofcom CEO report: http://www.ofcom.org.uk/about/accoun/reports_plans/annrep0506/ceo_rpt/, accessed 24 March 2007; see also http://www.out-law.com/page-5995, accessed 24 March 2007.
[51] *Ibid.,* see fn 37.
[52] See generally http://en.wikipedia.org/wiki/Enterprise_Risk_Management, accessed 24 March 2007.
[53] Globally, the preferred risk management module is enterprise risk management. See generally http://en.wikipedia.org/wiki/Enterprise_Risk_Management, accessed 24 March 2007.
[54] See generally http://www.admin.ox.ac.uk/riskmgt/overview.shtml, accessed 24 March 2007.
[55] Frederic Thiesse, "Managing risk perceptions of RFID" Auto-ID Labs White Paper WP-BIZAPP-031, pp 11-17; see Atkinson, W. (2004), "Tagged: the risks and rewards of RFID technology" Risk Management Journal 51 (7) at pp. 12-19; see also Cavoukian, A. (2004), "Tag, You're it: privacy implications of Radio Frequency identification Technology, Information and Privacy Commissioner Ontario, Toronto; see also an interesting Australian perspective: http://www.privacy.gov.au/news/04_07.html, accessed 24 March 2007.
[56] RFID risk manual can only be established once organisations or companies have undergone the levels of risk management exercise. See also an example of risk management checklist: http://www.lms.ca/@pdf/Risk_Management_Checklist.pdf, accessed 24 March 2007.

Appropriately, RFID risk manual should also incorporate the privacy risk checklist[57] that could serve as useful guidance and tool for the players. It is emphasized that the checklist should be based on the risk appetites of organisations and companies.

The option to adopt this legal risk management strategy is an open option. It is not meant to compel organisations and companies to adopt the same in the absence of a clear privacy and data protection provisions in Malaysia. Apropos, this option should also be taken into consideration as a means of internal control and thus, complementing privacy and data protection terms of other countries. There may be two potential arguments that underpin the adoption of legal risk management strategy, besides the typical cost and resources arguments. First, one may argue that there are also other technical standards that could mitigate such RFID related privacy risks. However, to counter argue that, it should be borne in mind that such existing standards are restricted on specific technology adoption and the risk assessment which is featured within any existing standards do not, in most cases, carry the levels of risk management in a whole package. Second, one may also argue that relying on data protection terms are sufficient to overcome privacy issues and there is no need to extend such existing standards or models to examine the level of privacy and data protection within RFID technology. To the contrary, the purpose of legal risk management model is to add the value to privacy and data protection provisions. It does not, however, lead to duplication and interface other existing standards or models and legal risk management is deemed to be pragmatic in mitigating the issues between RFID and privacy. Besides being the added value tool towards privacy and data protection, this model adopts the commendable practice is corporate governance.

5.4 Pre-empted compliance cost strategy

For RFID players, budgeting and spending towards regulatory compliance requires strategic planning. It should be pre-determined at an early stage to ensure the level of execution and implementation will take place without hindrance. A successful compliance cost strategy should involve dynamic participation of a team comprising of financial manager, human resource manager, risk manager, legal manager, internal auditor, project manager and corporate communications manager. The latter's composition only suits companies and organisations which have the required resources and control. However, for semi medium sized industries, the role could be managed by the director of the company or their supporting resources. It is undeniable that implementing a new legislation requires cost and thus, strategic budget planning should be effectively analysed and planned. This is to ensure that the players, organisations and companies are aware of the significant impact with the PDP Bill compliance cost requirements. The next step to ponder is the ability of RFID players to adopt a defensible and solid compliance cost strategy. This is deemed to be the challenging aspect in Malaysian contour. It is generally argued that such compliance cost which is resulted by new legislation in Malaysia does not tend to be friendly to small companies. However, it is submitted that due to the embryonic growth of Malaysia's privacy and data protection regime, these companies should be able to pre-empt and predict an informed analysis and decision to ensuring that cost shall not be the main hindrance towards their business continuity.

6. Conclusion

Whilst this paper is being finalised, the EU has just celebrated its 50th Anniversary.[58] The key speech on "A stronger Europe for a successful globalisation"[59] has further affirmed the EU's presence in legal and technology harmonisation. As reiterated, the PDP Bill should not be delayed as Malaysia's multilateral trade arrangements and investment with her EU partners

[57] See generally http://cyber.law.harvard.edu/ecommerce/privacyaudit.html, accessed 24 March 2007; see also http://www.itcinstitute.com/display.aspx?id=2499, accessed 24 March 2007.

[58] See http://news.bbc.co.uk/1/hi/world/europe/6490437.stm, accessed 26 March 2007; see also http://ec.europa.eu/commission_barroso/president/focus/50th_en.htm, accessed 26 March 2007.

[59] See http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/07/185&format=HTML&aged=0&language=EN&guiLanguage=en, accessed 26 March 2007.

looks promising and encouraging.[60] Whilst the EU has realised that the need to pass the PDP Bill is about time, it is submitted that emerging technology like RFID should not be anyway inhibit privacy and Malaysia's business growth if selected strategies by the RFID players are in place. For the proposed regulator, it is submitted that the drafting process of privacy and data protection provisions should also consider the market and regulatory trends that rely on technology neutrality and balanced harmonisation. On that note, it will be interesting and useful for the proposed regulator to ascertain the outcome of the EU RFID policy consultation[61] in the very near future.

[60] See generally http://ec.europa.eu/comm/external_relations/malaysia/intro/index.htm, accessed 26 March 2007.

[61] *Ibid.,* see fn 26.